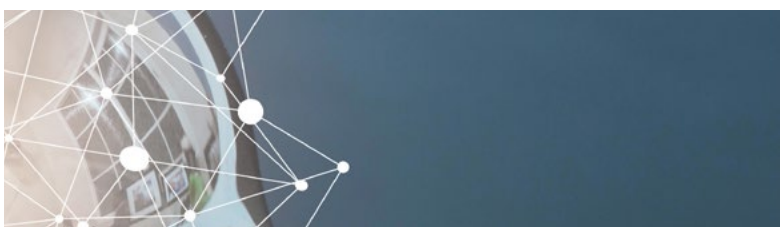
Digitale Lösungen: Wie kann die erforderliche Qualität sichergestellt werden?

Die Verantwortung für die Qualität digitaler Lösungen nimmt neue Dimensionen an

Die digitale Entwicklung schreitet rasant voran – in unserem Berufs- und Privatleben. Oftmals nutzen wir nur einen Teil der verfügbaren Lösungen und dennoch sind wir ständig auf der Suche nach etwas Neuem. Gleichzeitig treibt der zunehmend schnellere «Technologieschub» den Wandel laufend voran. Mit dem Beginn der COVID-19-Pandemie zeigte sich 2020, dass digitale Lösungen die einzige Möglichkeit sind, um in räumlich voneinander entfernten Umgebungen ein funktionsfähiges Arbeits- und Kommunikationsumfeld aufrechtzuerhalten. Diese Entwicklung wirft jedoch einige drängende Fragen auf: Woher wissen wir, dass die digitalen Anwendungen und Lösungen sicher genug sind? Sind beispielsweise von Algorithmen generierte Antworten ehrlich und gerecht? Sind wir gut genug gegen Cyberangriffe gerüstet? Geben wir unser Geld für die richtigen digitalen Lösungen aus?

All dies sind äusserst wichtige Fragen für Geschäftsleitungs- und Verwaltungsratsmitglieder, die in der Lage sein müssen, im jährlichen Berichtszyklus Rechenschaft über ihre Entscheidungen abzulegen. So könnte der Verwaltungsrat in seinem Bericht ausdrücklich auf die digitale Agenda und deren Qualität eingehen. Einige EU-Länder denken sogar bereits darüber nach, ob ein (externer) IT-Audit mit «Prüfbericht» Pflicht werden sollte. Die Verantwortung für die Qualität digitaler Lösungen nimmt angesichts der rasanten Entwicklung und der Tatsache, dass jeder mit jedem vernetzt ist, neue Dimensionen an. Auf dieser digitalen Autobahn wünschen wir uns alle mehr Sicherheit.

Auch in der Gesellschaft spielen diese Fragen eine Rolle. Beim Schutz der Privatsphäre besteht erheblicher Druck. Mehrere schmerzliche Beispiele zeigen, wie der Einsatz von Algorithmen im öffentlichen Bereich Bürgerinnen und Bürgern ernsthaft geschadet hat. So haben Fragen rund um digitale Integrität, Ehrlichkeit, Gerechtigkeit und Sicherheit gesellschaftlich an Bedeutung gewonnen.



«Es ist effektiver und effizienter, die Kontrollen während der Einführung digitaler Lösungen anzupassen, als sie im Nachhinein zu reparieren.»

Interessant ist, dass eine vergleichsweise grosse Anzahl von Unternehmen mit einem komplexen Mix von Technologielösungen arbeitet, die teils aus älteren (Legacy-)Systemen und teils aus neuen Online-Lösungen (Front-Office) bestehen. Die Datenintegrität, Funktionsfähigkeit und Kontinuität all dieser Lösungen sowie die allgemeine Ausfallsicherheit sicherzustellen ist keine leichte Aufgabe. Schwierig ist womöglich auch die Entscheidung, welche Investitionen sinnvoll sind, ebenso wie die Eindämmung der Instandhaltungskosten für ältere Lösungen, während gleichzeitig alles nach Plan laufen muss.

Kurz gesagt, es wird Zeit, dass sich Geschäftsleitungen und Verwaltungsräte auf der digitalen Autobahn Sicherheit verschaffen. Wie können Verantwortung und Rechenschaft formell verankert werden? Welche Rolle spielt der Verwaltungsrat dabei? Wie können IT-Audits dabei Mehrwert schaffen?

Eine gute Governance ist ein Muss auf Verwaltungsratsebene

Die Verwaltung und Überwachung digitaler Lösungen kann nicht als selbstverständlich vorausgesetzt werden. Die Komplexität der Technologie ist unübersehbar, und die Kombination von Altsystemen und neuen digitalen Lösungen macht jegliche Bemühungen um Transparenz zunichte. Häufig verwalten mehrere Parteien einzelne Teile der Technologiekette, während die Qualitätsanforderungen nicht immer ausdrücklich formuliert sind.

Hier bedarf es einer guten Governance. Nach Auffassung von Professor Steven de Haes (Universität Antwerpen), der im Zuge seiner Forschung zur IT-Governance viele Erkenntnisse gewonnen hat, müssen Verwaltungsräte im Hinblick auf digitale Lösungen vor allem auf zwei Bereiche fokussieren:

- Der erste Bereich betrifft digitale Risiken und die Frage, ob sie bewirtschaftet werden. Diese Frage kann nur beantwortet werden, wenn ein Standard vorliegt, der als Grundlage für eine Prüfung dienen kann. Gemäss dem Rahmenwerk des Committee of Sponsoring Organizations of the Treadway Commission (COSO), das häufig für Governance-Fragen herangezogen wird, kann dafür in Teilen das internationale CoBiT-Rahmenwerk (Control Objectives for Information Technology) verwendet werden. Damit macht das Management deutlich, welche Kontrollstandards in und um die digitalen Lösungen gelten, und kann deren Gestaltung sowie deren operative Wirksamkeit bestimmen und überwachen.
- Der zweite Bereich betrifft die Strategie. Setzt das Unternehmen auf die richtigen digitalen Entwicklungen? Ist die Strategie für den Einsatz digitaler Lösungen richtig? Sind die erforderlichen Investitionen angemessen? Diese Fragen können nur durch eine gründliche Analyse der Unternehmensziele und der erforderlichen digitalen Lösungen beantwortet werden, wobei der Schwerpunkt auf Effektivität und Effizienz liegen muss.

Oftmals wird ein stufenförmiges Modell angewandt, um die verschiedenen Verantwortlichkeiten auf mehreren Ebenen zu organisieren:

- Die erste Führungsebene definiert und überwacht die ordnungsgemässe Nutzung digitaler Lösungen. Eine Risiko- und Kontrollfunktion kann als zweite Ebene bei der Festlegung und Anwendung der richtigen Kontrollen sowie bei der Durchführung von Risikobewertungen hilfreich sein.
- Diese Ebene kann auch Formen der Überwachung der ordnungsgemässen Umsetzung und Nutzung der digitalen Lösungen organisieren.
- Eine interne Auditfunktion kann dann – als dritte Ebene – beurteilen, ob die Kontrollen in und um die digitalen Lösungen ordnungsgemäss eingerichtet wurden und wirksam sind. Falls gewünscht, kann dies auch durch eine externe (IT-)Auditfunktion bestätigt werden.

Der Verwaltungsrat ist dafür verantwortlich, dass dieses mehrstufige Governance-Modell etabliert und überwacht wird. Er kann jederzeit unabhängige Bewertungen durch (IT-)Prüfer anordnen, um sich Gewissheit zu verschaffen.

Angesichts des raschen digitalen Wandels müssen die Kenntnisse über Technologie ständig aktualisiert werden. Zu einer guten Governance gehört auch, diesen Aspekt zu organisieren und zugleich die Qualität der Lösungen – sowie allfällige damit verbundene Beschränkungen – zu berücksichtigen. Governance ist keine statische Aufgabe: Veränderungen in der digitalen Kette müssen fortlaufend bewertet und nötigenfalls angepasst werden. Wendet sich das Blatt? Oder mit anderen Worten: Sind die neuen digitalen Lösungen mittlerweile so komplex, dass niemand mehr beurteilen kann, ob ihr Inhalt richtig oder angemessen ist? Vom Standpunkt der Managementverantwortung aus gesehen ist es keine gangbare Option, sich für einen solchen «Black Box»-Ansatz zu entscheiden. So können wir beispielsweise nicht zulassen, dass Algorithmen verwendet werden, deren Richtigkeit und Gerechtigkeit wir nicht überprüfen konnten.

IT-Audits und -Standards

Bei einem IT-Audit geht es um eine unabhängige Beurteilung der Qualität der Informationstechnologie (Prozesse, Governance, Infrastruktur) oder, wie oben erwähnt, der digitalen Lösungen. Dadurch wird der Audit zu einem wichtigen Instrument, das bei der Entwicklung und Anwendung digitaler Lösungen Sicherheit bieten oder Risiken erkennen kann. Der IT-Prüfer verfügt über eine Reihe von Instrumenten, mit denen er die digitalen Lösungen unter mehreren Qualitätsgesichtspunkten überprüfen kann. Eine zunehmende Anzahl von Prüfungs- und Berichtsstandards ermöglicht es, Kunden Garantien oder ein genaues Bild ihrer Risiken zu verschaffen. Zu den bedeutendsten Standards gehören:

- International Standards on Assurance Engagements (ISAE) 3402

Dieser Standard wurde aus Prüfungssicht entwickelt, damit sich der Abschlussprüfer des Kundenunternehmens beim Outsourcing eines Audits über die Qualität der von einem Dienstleistungsunternehmen geleisteten Arbeit informieren kann.

- Service Organization Control 1 (SOC-1)

Bei SOC-1 (oder ISAE 3402) liegt der Schwerpunkt auf der Zuverlässigkeit und Kontinuität der Finanzdatenverarbeitung. SOC-2 deckt ein breiteres Spektrum von Qualitätsaspekten (wie Datenschutz) und Datenflüssen ab.

- Bericht nach ISAE 3000

ISAE 3000 ist ein weiterer Assurance-Bericht, mit dem nachgewiesen werden soll, dass die von einem Unternehmen vorgesehenen internen Managementprozesse wie beschrieben durchgeführt werden. Der Bericht (der auch als SOC-2 bezeichnet wird) kann sich auf viele Themen beziehen und deckt verschiedene Qualitätsaspekte wie Vertraulichkeit und Datenschutz ab.

- Bericht nach ISAE 4400

Bei dieser Variante handelt es sich um einen Bericht über vereinbarte Verfahren. Wer den Bericht liest, muss sich eine eigene Meinung über die Tätigkeiten und Feststellungen bilden, die der IT-Prüfer darin darstellt.

In den letzten Jahren hat sich im Bereich des IT-Audits viel getan, unter anderem in der Bewertung von Algorithmen und entsprechenden Erklärungen. Ein Beispiel ist die Frage der Gerechtigkeit und Unvoreingenommenheit von Daten. Um das Risikobild komplexer digitaler Lösungen zu verstehen und Gewissheit zu schaffen, muss die Wechselwirkung von mehreren Disziplinen berücksichtigt werden. So arbeiten IT-Prüfer bei der Prüfung von Algorithmen mit Datenspezialisten und Juristen zusammen.

Schlussbemerkungen

Anhand der aktuellen Standards für IT-Audits können bereits viele Fragen zu digitalen Lösungen beantwortet werden, die sich der Verwaltungsrat stellen muss. IT-Prüfer sollten klar kommunizieren, was sie tun können, und mit den Aufsichtsbehörden zusammenarbeiten, um ihr Arsenal an Instrumenten zu erweitern. Ihre Sprache und Erklärungen müssen manchmal vereinfacht werden, um deutlich zu machen, was wirklich vor sich geht. Der Verwaltungsrat kann und muss seine Fragen verfeinern und selbst Verantwortung übernehmen, beispielsweise indem er angemessene Kontrollen gewährleistet.

Secure-by-Design dürfte zunehmend zur Norm werden, da auch Technologieanbieter verstehen, dass bei der Entwicklung neuer Lösungen die richtigen Kontrollen umgesetzt werden müssen. Einige Anbieter sehen auch Mechanismen vor, die eine kontinuierliche Überwachung gewährleisten. Dabei wird geprüft, ob die vorhandenen Kontrollen durchweg ordnungsgemäss funktionieren, und Ausnahmen werden gemeldet. Auch in diesem Zusammenhang spielt das Management eine wichtige Rolle bei der Umsetzung der oben beschriebenen Grundsätze. Es ist effektiver und effizienter, die Kontrollen während der Einführung digitaler Lösungen anzupassen, als sie im Nachhinein zu reparieren.

Je mehr ein Unternehmen zu einer kontinuierlichen Überwachung übergeht, desto eher kann der IT-Prüfer zu einer Form des kontinuierlichen Audits übergehen, bei denen jederzeit Informationen über den Einsatz der digitalen Lösung eingeholt werden können. Dieser Ansatz würde die Agenda des Verwaltungsrats in Zukunft noch stärker unterstützen.

Prof. Dr. Rob Fijneman
Partner, Audit

+41 58 249 23 27
robfijneman@kpmg.com

Erkenntnisse von Professor Dr. Rob Fijneman RE RA
Dieser Beitrag basiert auf einer Kombination aus Forschungserkenntnissen, Ergebnissen von Masterarbeiten und praktischen Erfahrungen aus IT-Audits. Rob Fijneman ist Professor für IT Auditing an der TIAS School for Business and Society/Universität Tilburg. Gleichzeitig ist er als Partner im Bereich Technologie-Audits für die KPMG AG in der Schweiz tätig. Seine Erfahrung beruht auf einem breiten Spektrum an Prüfungs- und Beratungsdienstleistungen, die er in den letzten 36 Jahren für multinationale Kunden erbracht hat. 2019 wurde er vom niederländischen König für seine Leistungen im Bereich IT Auditing zum Offizier im Orden von Oranje-Nassau ernannt.

Dieser Artikel ist Bestandteil der KPMG Board Leadership News. Um diesen Newsletter für Verwaltungsrätinnen und Verwaltungsräte dreimal pro Jahr zu erhalten, können Sie sich hier registrieren.

Über das KPMG Board Leadership Center

Das KPMG Board Leadership Center ist unser Kompetenzzentrum für Verwaltungsrätinnen und Verwaltungsräte. Mit vertieftem Fachwissen und neusten globalen Kenntnissen unterstützen wir Sie in Ihren aktuellen Herausforderungen, damit Sie Ihre Rolle höchst effektiv erfüllen können. Zusätzlich bieten wir Ihnen die Möglichkeit, mit Gleichgesinnten in Kontakt zu treten und sich auszutauschen.

Erfahren Sie mehr unter kpmg.ch/blc.